KPMG JOANNEUM RESEARCH SILICONALPS

11 AUSGABE CYBERSECURITY STUDIE

Cybersecurity in Österreich 2026

Sicherheitsforum
Digitale Wirtschaft
Österreich

Lagebild Cybersecurity 2026

—

Graz, 11. Juni 2026

Cybersecurity in Österreich 2026

1 **Rückblick und aktuelles Lagebild**
Die Fähigkeit von Unternehmen, Vorfälle zu erkennen, ist so wichtig, wie nie zuvor

2 **Cyberregulatorik und Umsetzung von NISG 2026**
Welche konkreten Anforderungen an Governance, Prozesse und Nachweisfähigkeit sich daraus ergeben

3 **Künstliche Intelligenz**
Ein eigenständiger Einflussfaktor in der digitalen Risikolandschaft

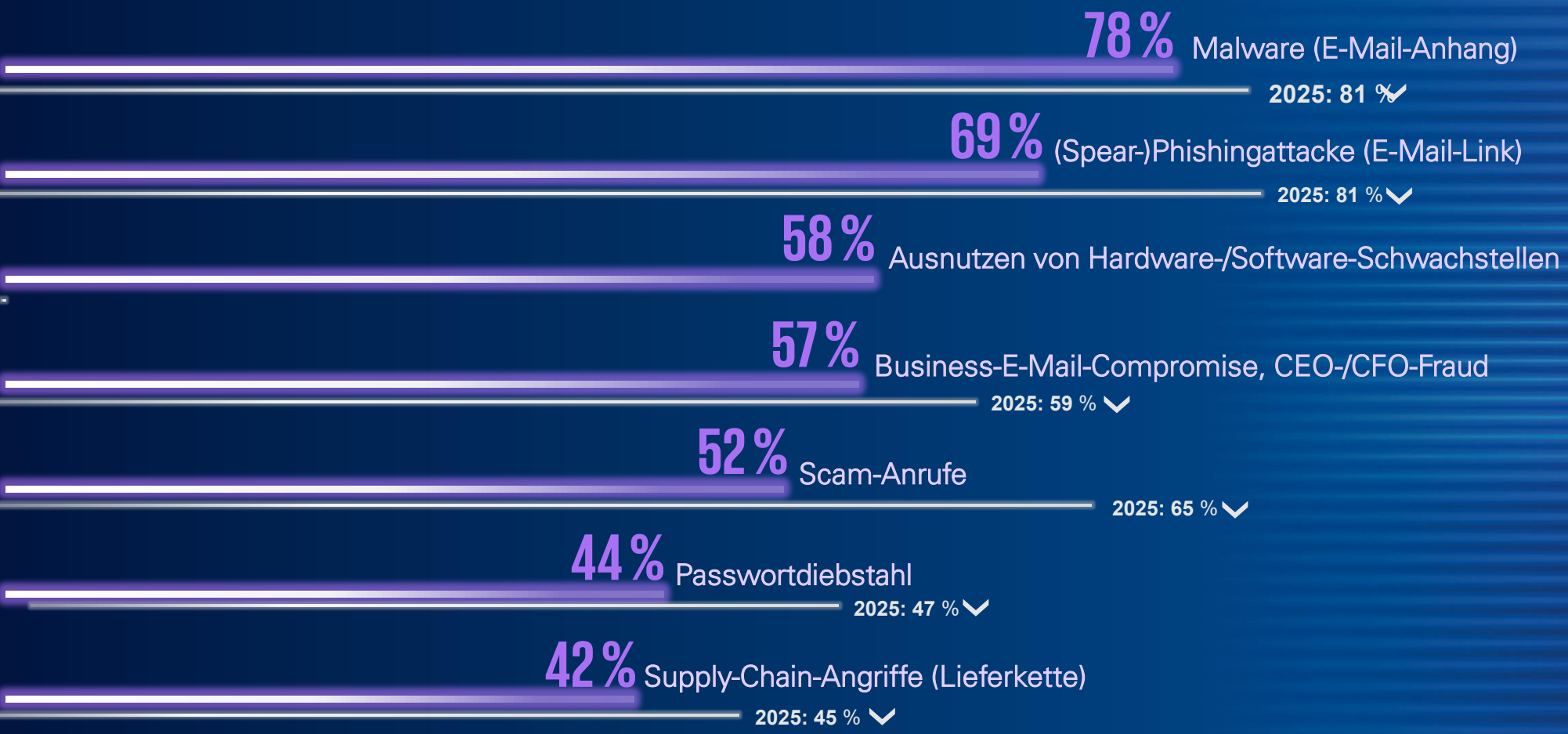
4 **Digitale Souveränität**
Vom bloßen politischen Schlagwort zu einer zentralen Strategiefrage für Wirtschaft, Staat und Gesellschaft

5 **Ausblick**
Die Cybersecurity-Agenda heimischer Unternehmen

Rückblick und aktuelles Lagebild

Die Fähigkeit von Unternehmen, Vorfälle zu erkennen, ist so wichtig, wie nie zuvor

Top 7 Angriffsarten 2026



Zu- und Abnahmen in den letzten 12 Monaten

+58 % Ausnutzen von Hardware-/ Software-Schwachstellen

+9 % Industrieanlage angegriffen (OT)

+8 % Cloud-Fehlkonfiguration

+8 % MFA-Bypass

+4 % Insider Threat

Denial-of-Service-Attacken (DoS) **-15 %**

Scam-Anrufe **-13%**

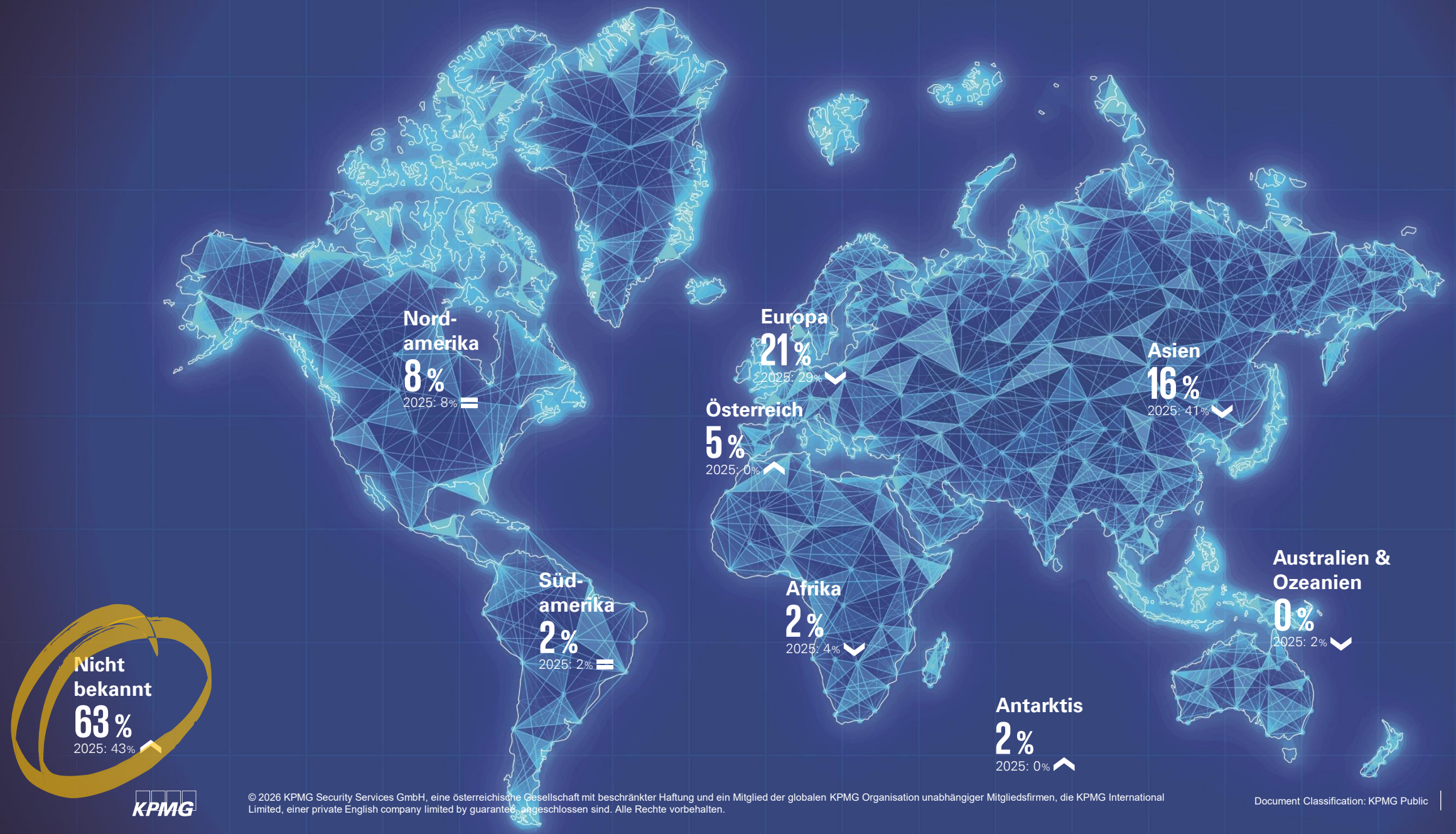
(Spear-)Phishing-attacke (E-Mail-Link) **-12%**

Advanced Persistent Threats (APTs) **-10%**

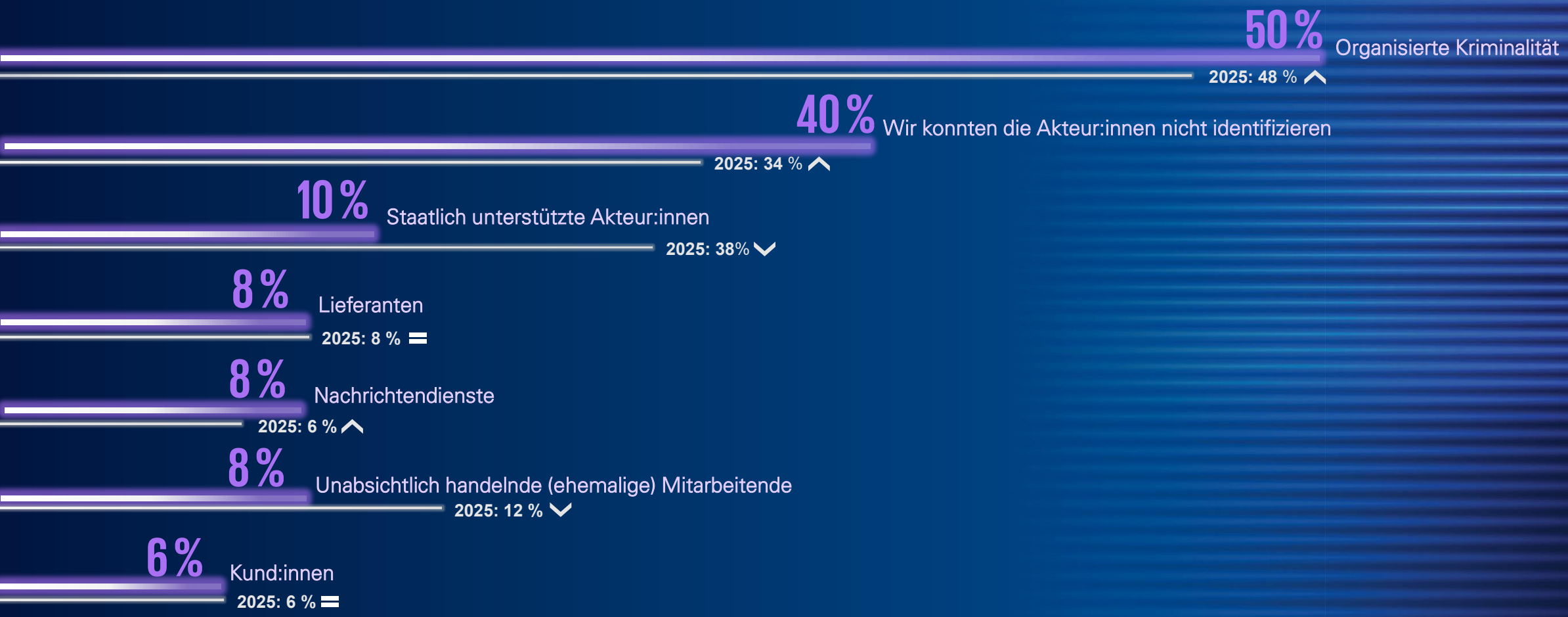
Spoofing **-10%**

Branchen im Fokus im Vergleich

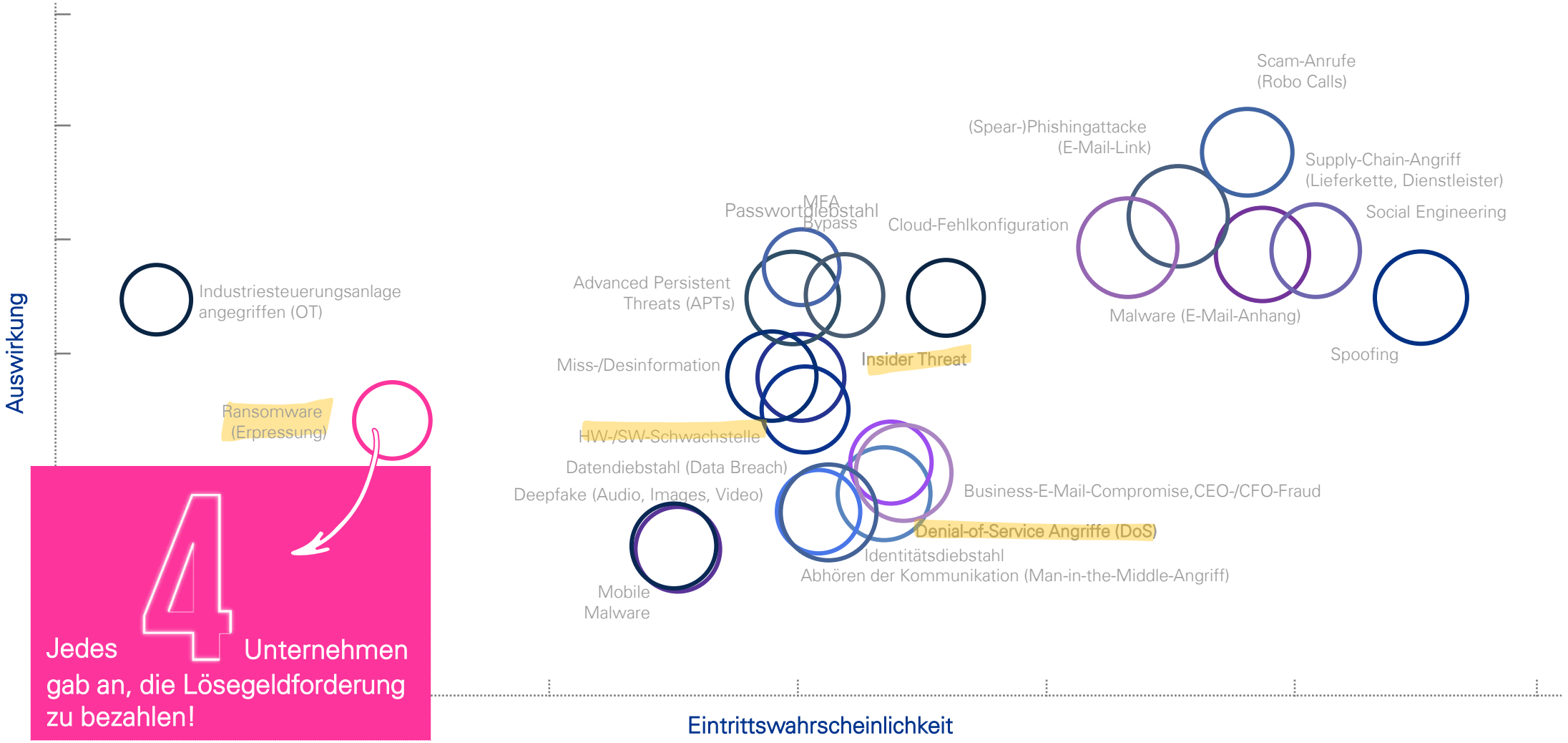
	2025		2026
Automobilindustrie		1	Automobilindustrie
Energiewirtschaft		2	Tourismus
Chemiewirtschaft		3	Energiewirtschaft
Öffentlicher Sektor		4	Konsumgüter
Tourismus		5	Lebensmittel



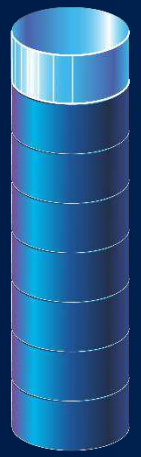
Akteur:innen von denen die Angriffe ausgingen



Eintrittswahrscheinlichkeit und Auswirkung 2026

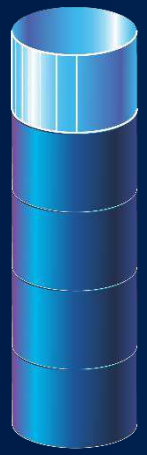


Key Findings Cybersecurity-Studie 2026



Jeder **8.** Cyberangriff **war** in den letzten 12 Monaten **erfolgreich**.

30% der Cyberangriffe führten zu einem länger andauernden **Unternehmensstillstand**.

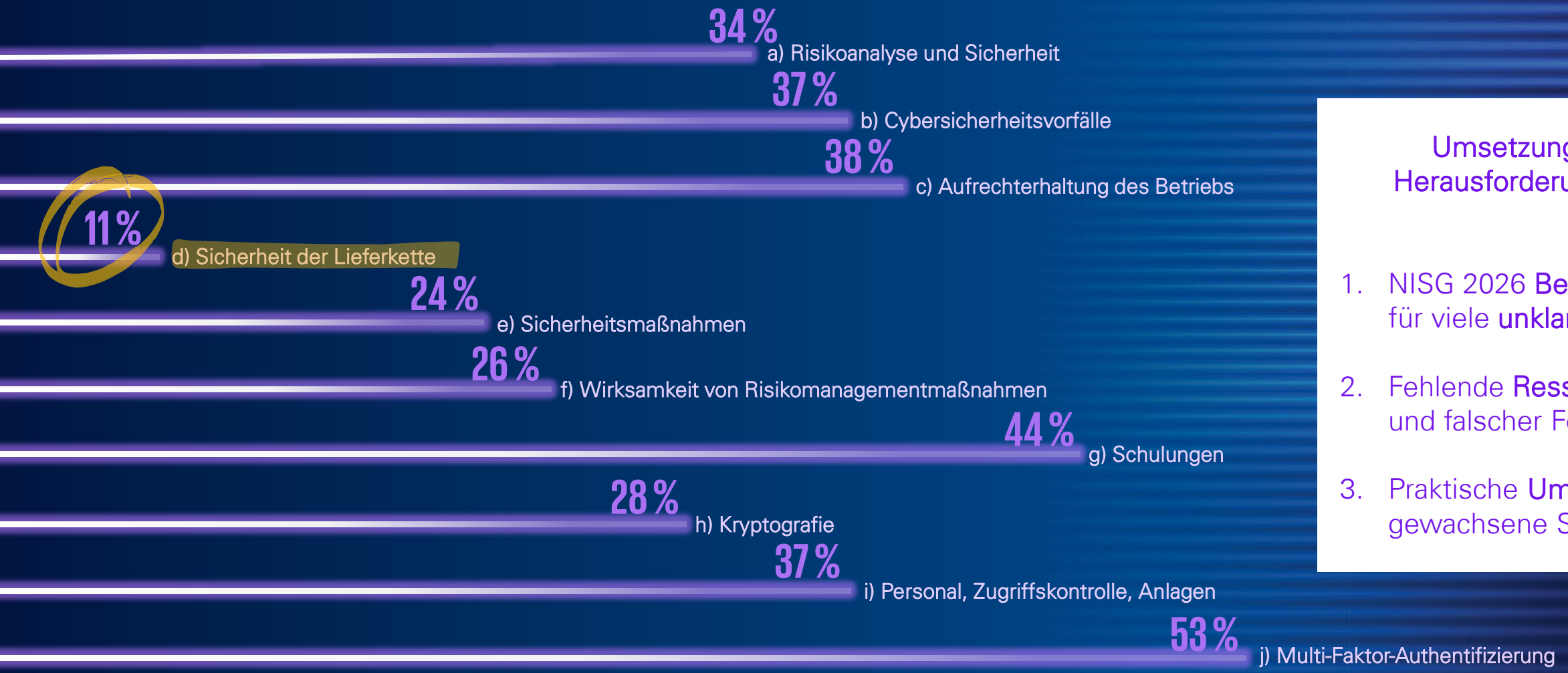


Jeder **5.** Cyberangriff fand **über die Lieferkette** statt.

Cyberregulatorik und Umsetzung von NISG 2026

Welche konkreten Anforderungen an Governance, Prozesse und Nachweisfähigkeit sich daraus ergeben

NISG 2026 Netz- und Informationssystemsicherheitsgesetz 2026



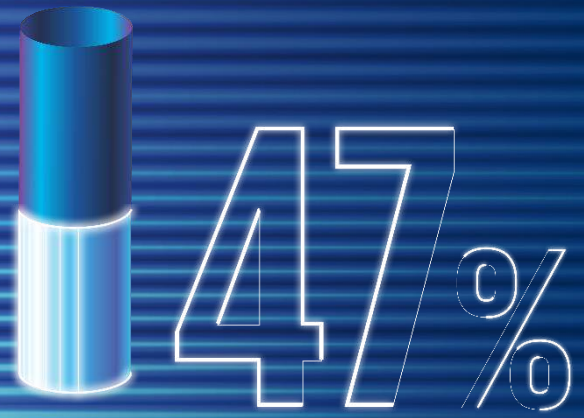
Umsetzungs-Herausforderungen

1. NISG 2026 **Betroffenheit** für viele **unklar**
2. Fehlende **Ressourcen** und falscher Fokus
3. Praktische **Umsetzung,** gewachsene Strukturen

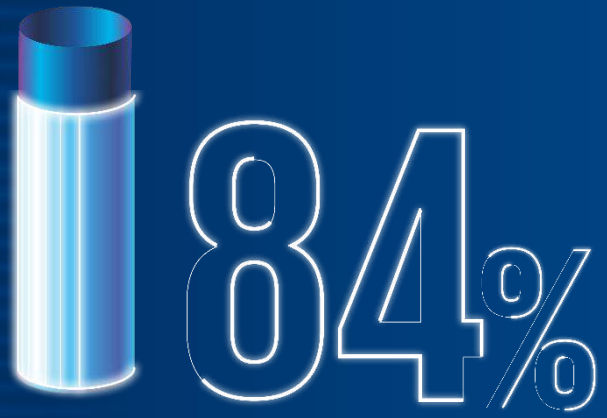
Künstliche Intelligenz

Ein eigenständiger Einflussfaktor in der digitalen Risikolandschaft

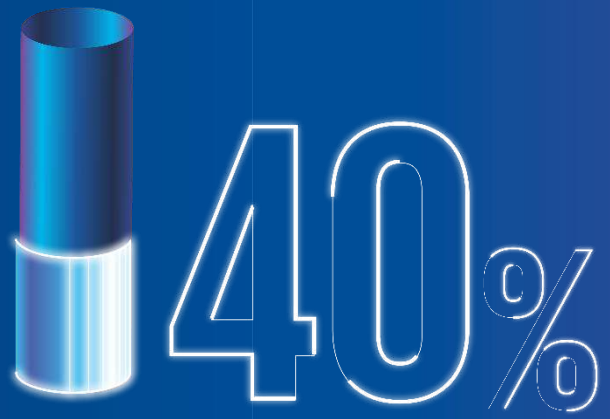
Künstliche Intelligenz verändert die Spielregeln



geben an, dass bereits **verstärkt KI** bei der **Durchführung von Cyberangriffen** gegen ihr Unternehmen eingesetzt wird.

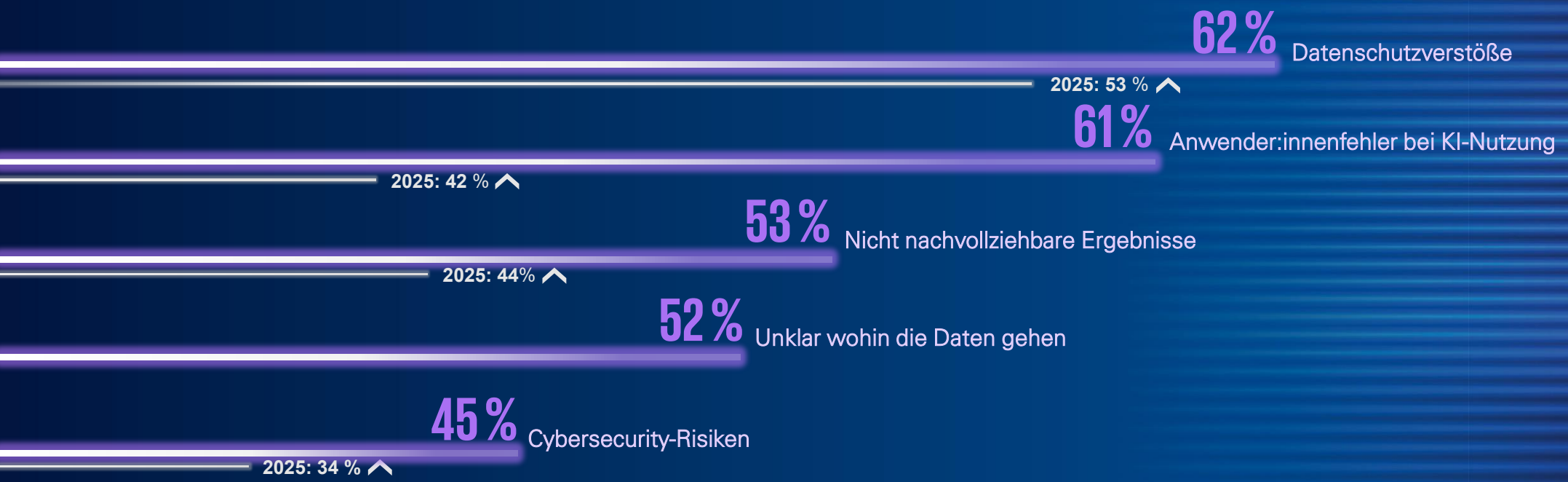


Bei 84% hat die Künstliche Intelligenz die **Bedrohungslage** durch Cyberangriffe **verschärft**.



In 40% der Fälle war **ineffektives Patchmanagement** das häufigste Einfallstor.

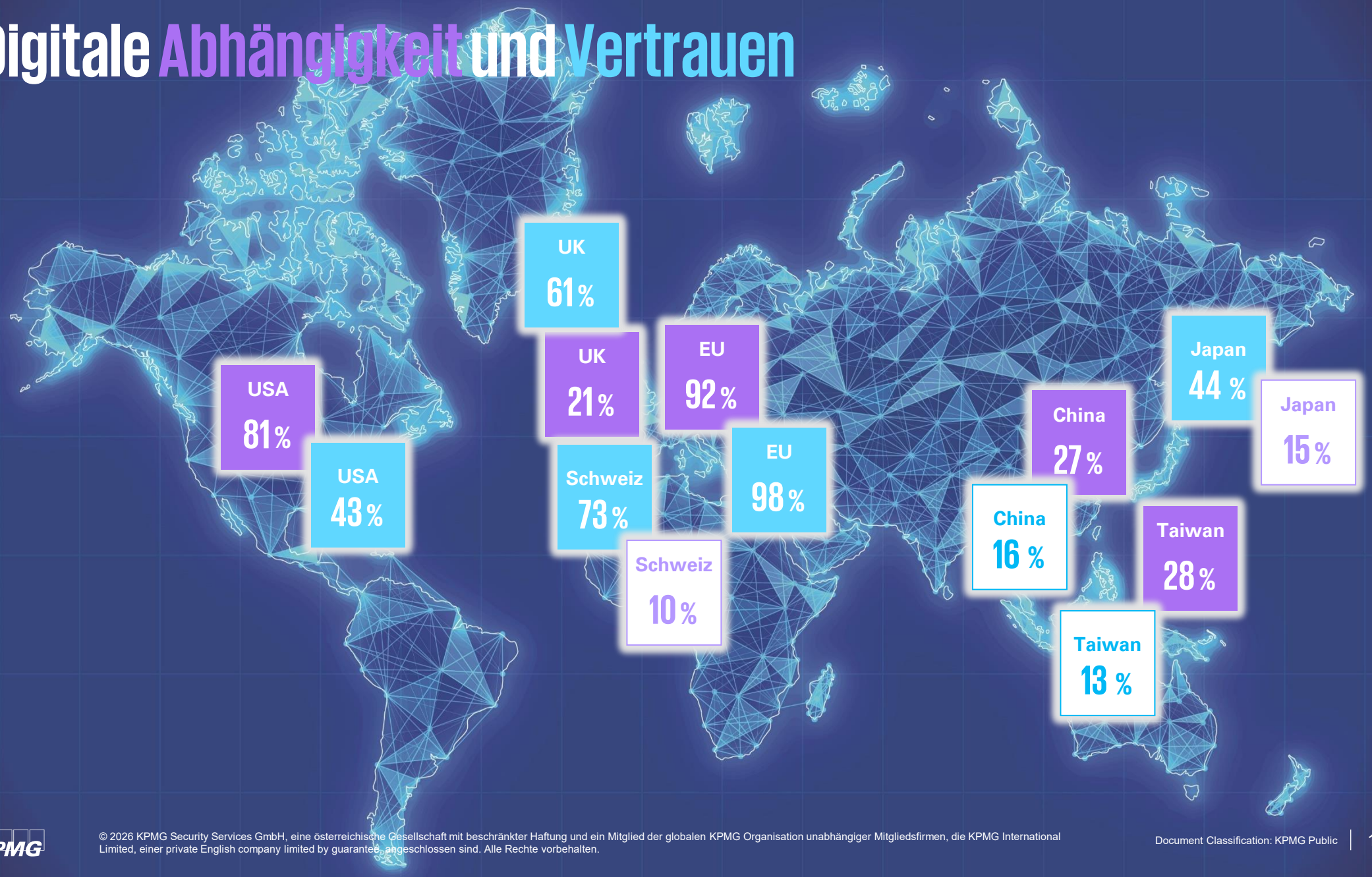
Künstliche Intelligenz verändert die Spielregeln



Digitale Souveränität

Vom bloßen politischen Schlagwort zu einer zentralen Strategiefrage für Wirtschaft, Staat und Gesellschaft

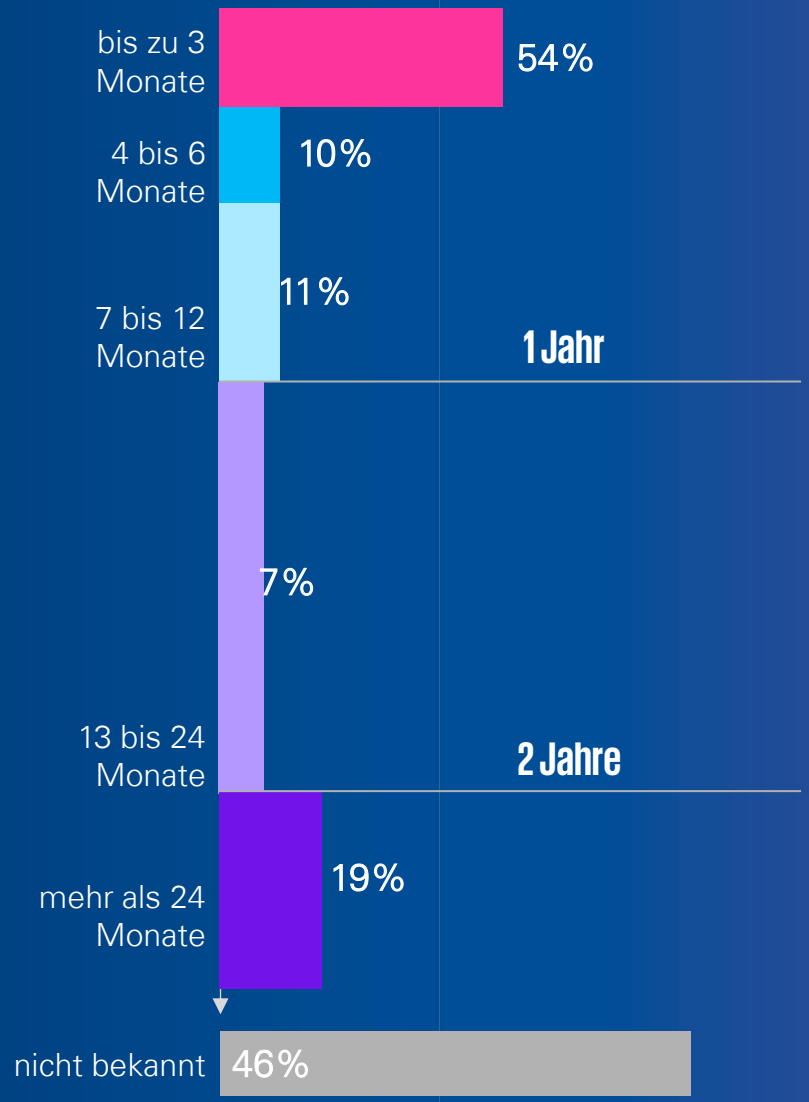
Digitale Abhängigkeit und Vertrauen



Digitale Abhängigkeit

70% der Unternehmen sehen eine hohe technologische Abhängigkeit.

69% können die Abhängigkeit von ausländischen Geschäftspartnern aktuell nicht umgehen.

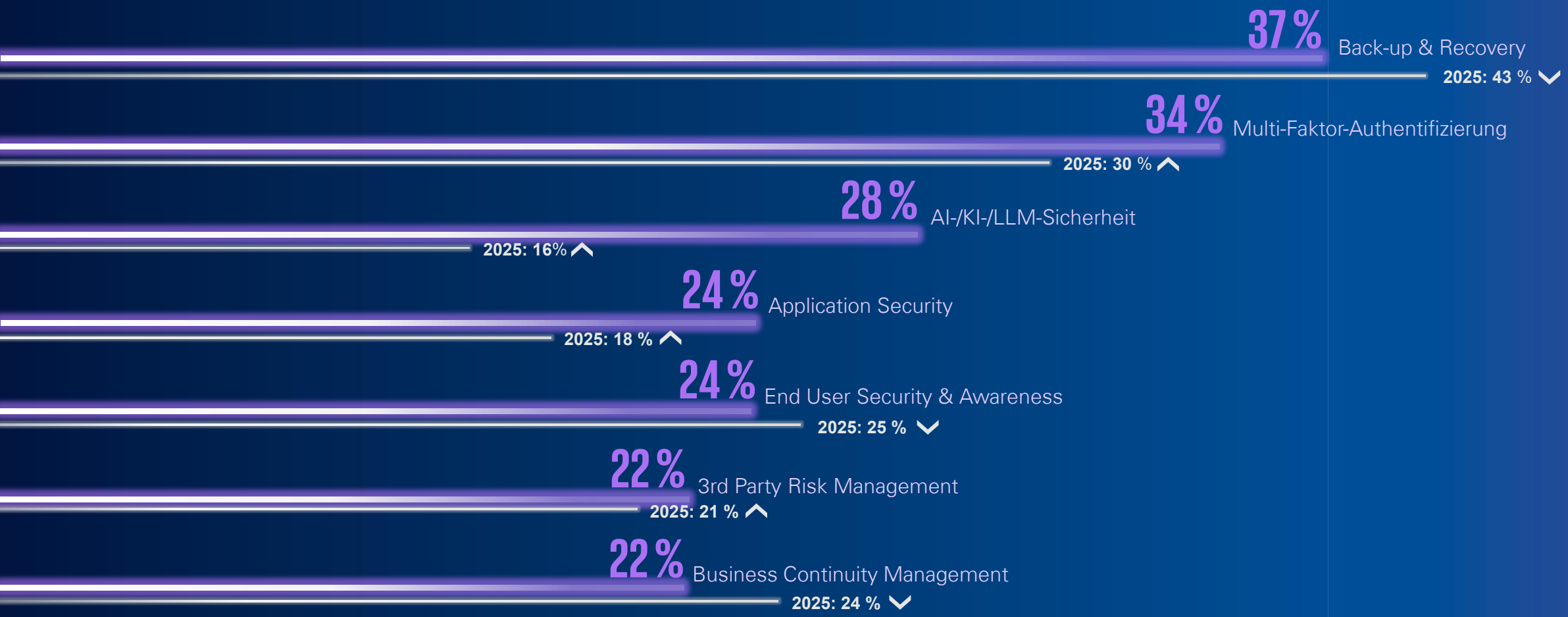


Ausblick

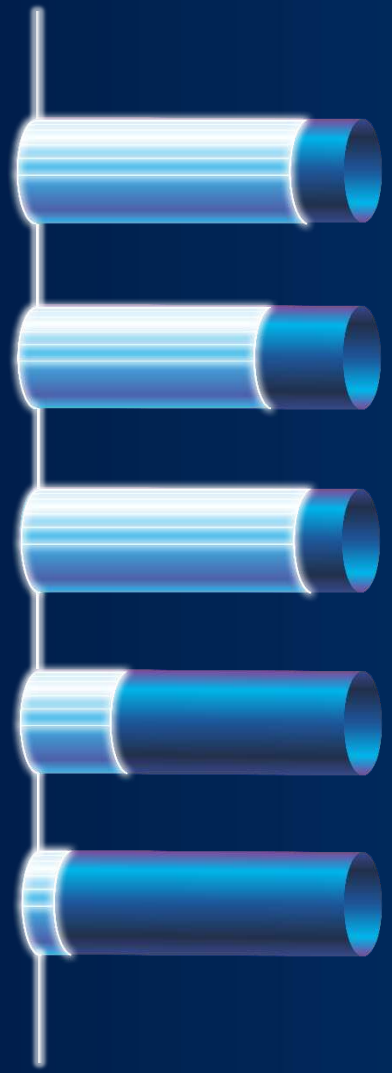
Die Cybersecurity-Agenda heimischer Unternehmen

5

Maßnahmen in den kommenden 12 Monaten



Cybersecurity Reality Check



83 % würden bevorzugt Security-Lösungen von österreichischen Unternehmen einsetzen.
(2025: 60 Prozent)

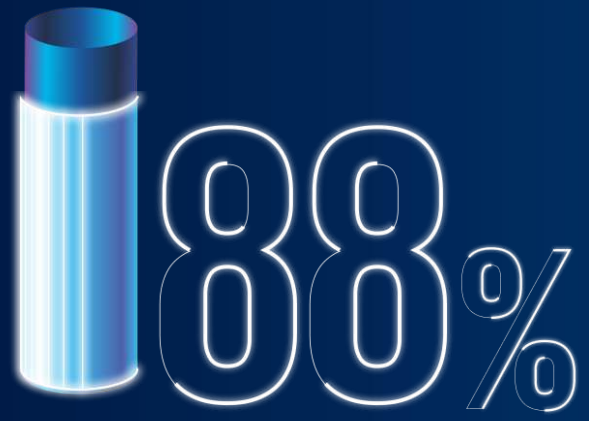
74 % sagen, dass heimische Cybersecurity-Unternehmen von der Politik gezielt gefördert werden sollten.
(2025: 69 Prozent)

89 % sind der Meinung, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt.
(2025: 88 Prozent)

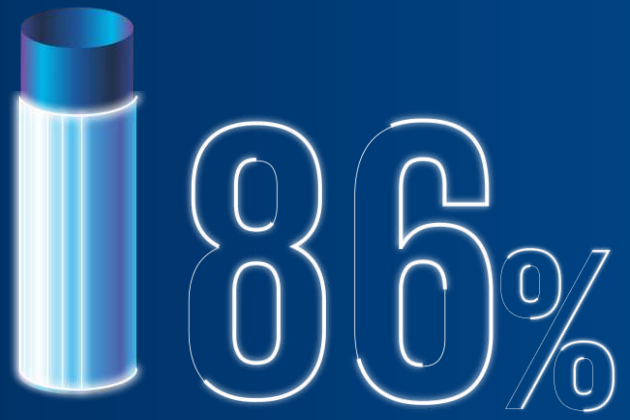
28 % glauben, dass Österreich in der Lage sein muss, selbst Cyberangriffe durchzuführen.
(2025: nicht erhoben)

15 % Lediglich 15 Prozent sind zuversichtlich, dass Österreich gut darauf vorbereitet ist, auf schwerwiegende Cyberangriffe auf die kritische Infrastruktur zu reagieren.
(2025: 13 Prozent)

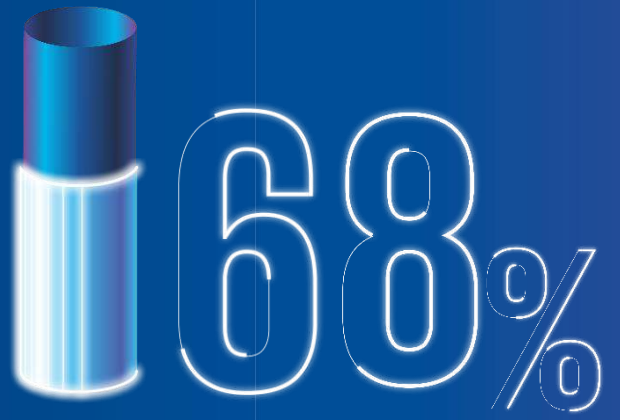
Cybersecurity Reality Check



stufen den Cyberraum als **primäre Dimension** künftiger Konfliktführung ein.



fordern robuste defensive Fähigkeiten der Republik im digitalen Raum



finden, dass es eine operative **Gleichstellung von Cyberoperationen** mit konventionellen militärischen Angriffen braucht.

11. AUSGABE
CYBERSECURITY
STUDIE

Cybersecurity ist keine Option. Sie ist Voraussetzung für wirtschaftliches und gesellschaftliches Überleben.

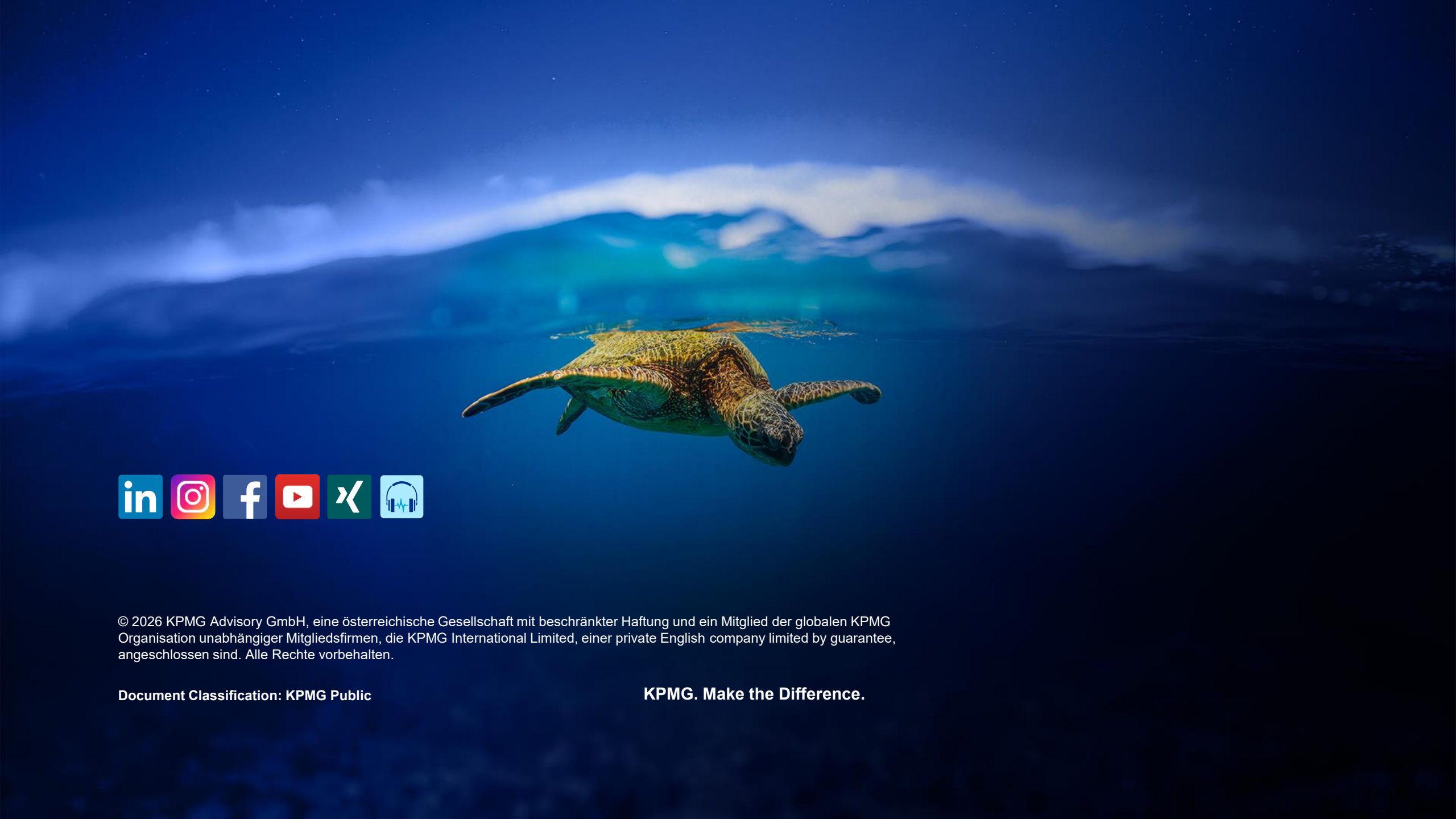
Die eigentliche Frage ist nicht, ob wir investieren, sondern ob wir es uns leisten können, es nicht zu tun.

Kontakt

Robert Lamprecht

Partner Cybersecurity & Crisis Management
T +43 1 31332-3409
M +43 664 816 12 32

rlamprecht@kpmg.at



Document Classification: KPMG Public

KPMG. Make the Difference.